PCT/EP 99/07019

BUNDESREPUBLIK DEUTSCHLAND

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	198 45 096.6
Anmeldetag:	30. September 1998
Anmelder/Inhaber:	Philips Corporate Intellectual Property GmbH, Hamburg/DE
Bezeichnung:	Verfahren zum gesicherten Ablegen von Daten in Speichern und Registern
IPC:	G 06 F, G 06 K
Bemerkung:	Die Anmelderin firmierte bei Einreichung dieser Patentanmeldung: Philips Patentverwaltung GmbH

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 11. Juli 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

A 9161
06/00
EDV-L

PHD 98-122

Titel: Verfahren zum gesicherten Ablegen von Daten in Speichern und Registern

Hintergrund:

In vielen Datenverarbeitungsgeräten werden zu deren geschützten Betrieb bzw. zum geschützten Transport der verwendeten Daten kryptographische Operationen eingesetzt. Die hierfür notwendigen Berechnungsoperationen werden dabei sowohl von Standard-, als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel hierfür stellt z.B. die Chipkarte dar.

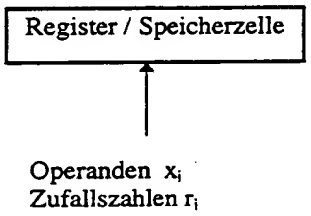
Im Vorfeld einer solchen kryptographischen Berechnung müssen in diesen Datenverarbeitungsgeräten oftmals Speicherbereiche bzw. Register mit Operanden initialisiert werden. Während der Berechnung werden ggf. Zwischenergebnisse in Speicherbereichen oder Registern abgelegt und auch abschließend wird das Ergebnis der Berechnung zur Weiterverarbeitung in Speicherbereichen oder Registern abgelegt. Bei den in diesem Zusammenhang verwendeten Operanden bzw. Zwischenergebnissen handelt es sich i.d.R. um sicherheitsrelevante Informationen (z.B. kryptographische Schlüssel).

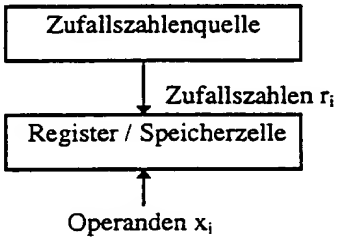
Abhängig von der verwendeten Technologie, führt das Laden der Speicherbereiche bzw. Register mit Daten zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie z.B. der CMOS-Technologie, hängt dieser erhöhte Verbrauch von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. D.h., daß das Laden eines zuvor gelöschten Registers den Strom proportional zum Hamminggewicht des Operanden (= Anzahl der Bits, mit dem Wert '1') ansteigen läßt.

Durch die Beobachtung dieser Stromänderung könnte, je nach ausgeführter Operation, ein Außenstehender wertvolle Informationen erhalten, mit deren Hilfe er eine erfolgreiche Kryptoanalyse der ausgeführten Operation durchführen könnte.

Gegenmaßnahme:

Als Gegenmaßnahme wird der Speicherbreich bzw. das Register zuvor mit einem geheimen Zufallswert initialisiert. Dieses Laden mit einem Zufallswert kann entweder durch das Rechenwerk selbst oder auch durch eine direkte Verbindung zwischen Zufallszahlenquelle und Register geschehen.





Der Zeitpunkt dieser Vorinitialisierung kann nun beliebig gewählt werden und muß nicht unmittelbar vor der kryptographischen Operation liegen. Auch eine wiederholte Vorinitialisierung der Speicherbereiche bzw. Register mit einem sich ändernden Zufallswert ist denkbar.

Werden die so vorinitialisierten Speicherbereiche bzw. Register im Zuge einer kryptographischen Operation mit Daten geladen, ändert sich der Stromverbrauch nun lediglich abhängig von der Differenz des Hamminggewichts des Operanden und des Hamminggewichts der unbekannten Zufallszahl.

Ausgehend von diesem Differenzwert ist es nun nicht mehr möglich, Angaben über die verwendeten Operanden bzw. Zwischenergebnisse abzuleiten.

Literatur:

P. Kocher, "Introduction to Differential Power Analysis and Related Attacks", www.cryptography.com/dpa

G.J. Simmons, "Contemporary Cryptology", IEEE Press, 1992